IN THE CLAIMS:

The following is a complete listing of the pending claims:

1. (Currently Amended) A method of decrypting data stored on a storage medium using an encryption/decryption core embedded on a data storage engine, the method comprising:

generating an internal key ~~using~~ within the data storage engine;

generating a combination key by combining a medium key with the internal key within the data storage engine; and

within the data storage engine, decrypting a first portion of data stored on the storage medium with said ~~first~~ combination key.

2. (Previously Presented) The method of Claim 1, further comprising

decrypting a master media key; and

generating the medium key from the master media key.

3. (Original) The method of Claim 1 wherein the internal key is generated by a pseudo-random number generator.

Claims 4 through 5 (cancelled)

6. (Original) The method of Claim 1 wherein the combination key is generated by combining the internal key with the medium key in an exclusive OR function.

7. (Previously Presented) The method of Claim 1 wherein the first portion is decrypted using triple DES for two keys, wherein a first key is the combination key and a second key is an additional internal key.

8. (Previously Presented) The method of Claim 2 wherein the medium key comprises a mastered system area key, a writable system area key, and a file system information key.

9. (Previously Presented) The method of claim 8 further comprising:

generating an additional internal key.

10. (Previously Presented) The method of Claim 9 wherein:

the first portion of data comprises mastered data;

generating a combination key further comprises combining the mastered system area key with the internal key in an XOR function; and

decrypting the first portion further comprises using triple DES with two keys, wherein the first key is the combination key and the second key is the additional internal key.

11. (Previously Presented) The method of Claim 9 wherein:

the first portion of data comprises unmastered data;

generating a first combination key further comprises combining the writable system area key with the internal key in an XOR function; and

decrypting the first portion further comprises using triple DES with two keys, wherein the first key is the combination key and the second key is the additional internal key.

12. (Previously Presented) The method of Claim 11 further comprising:

storing a second portion of data on said unmastered area; and

encrypting the second portion of data using single DES, wherein the key is the combination key.

13. (Previously Presented) The method of Claim 9 further comprising:

generating an additional combination key by combining the file system information key with the internal key in an XOR function;

decrypting a file system stored on the storage medium using the internal key;

decrypting a second portion of data using triple DES with a first and a second key, wherein the first key is an additional combination key and the second key is the additional internal key, the second portion comprising a plurality of file pointers linking a file system and the first portion of data.

14. (Currently Amended) A method of decrypting data using a data storage engine comprising a data buffer and an application specific integrated circuit (ASIC), the ASIC having an encryption/decryption engine and a pseudo-random number generator, and the data being stored on a storage medium, the method comprising:

generating a plurality of internal keys using the pseudo-random number generator;

decrypting a master media key and a directory structure corresponding to a first portion of the data using at least one internal key;

generating a plurality of medium keys from the master media key;

generating a plurality of combination keys from the plurality of medium keys and the plurality of internal keys; and

decrypting a first portion of the data with ~~using~~ a first combination key from the plurality of combination keys.

15. (Original) The method of Claim 14 wherein the pseudo-random number generator comprises a logical feedback shift register, and wherein "generating a plurality of internal keys" further comprises:

seeding the logical feedback shift register with a seed stored in the ASIC.

16. (Original) The method of Claim 14 further comprising:

decrypting a plurality of file pointers linking the directory structure to the data using a second combination key, wherein the plurality of decrypted file pointers is stored within the ASIC.

17. (Original) The method of Claim 14 further comprising:

encrypting said first portion.

18. (Original) The method of Claim 17 wherein:

said decrypting a first portion of data further comprises decrypting using triple DES with two keys, wherein a first key is the first combination key and the second key is a first internal key; and

said encrypting further comprises encrypting using single DES, wherein the key is a second internal key.

19. (Original) The method of Claim 17 further comprising

decrypting a second portion of the data using a second combination key, wherein the first portion comprises mastered data and the second portion comprises data saved by a user.

20. (Original) A method of encrypting data stored on a storage medium using an encryption/decryption core embedded on a data storage engine, the method comprising:

generating a plurality of internal keys using the data storage engine;

decrypting a master media key stored on the storage medium using at least one of the plurality of internal keys;

generating a plurality of medium keys from the master media key;

generating a first combination key by combining a medium key with an internal key;

encrypting a first portion of data using said first combination key;

storing the first portion on the storage medium.

21. (Original) The method of Claim 21 wherein encrypting a first portion further comprises encrypting using single DES.

Claims 22 through 25 (cancelled)